A Standard for Standards?

John Knight
Department of Computer Science
University of Virginia

Benefits of Standards

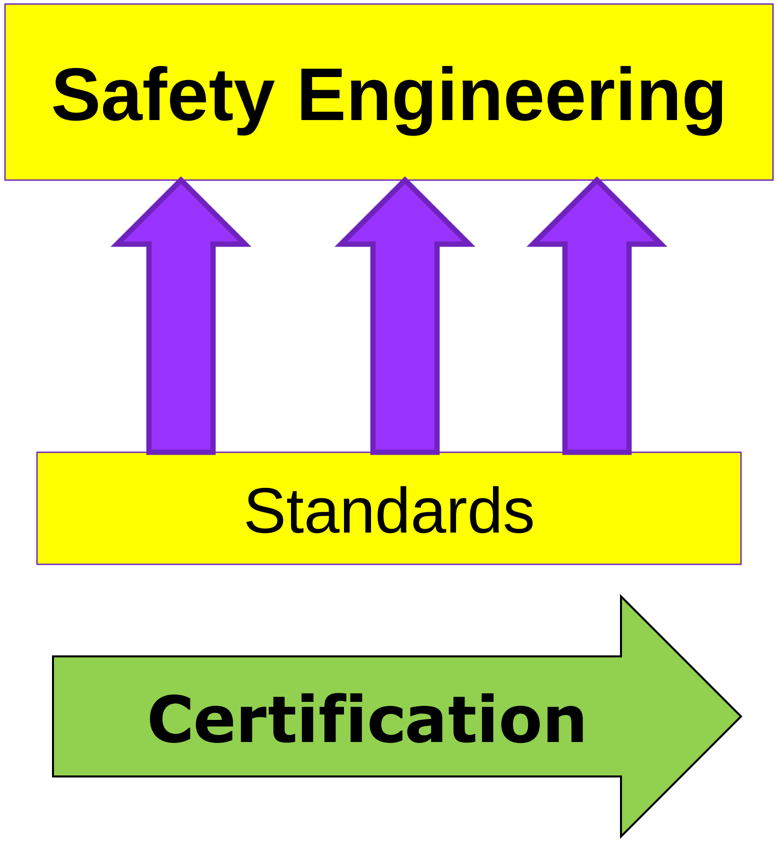
- Standards are immensely beneficial
- Benefits extend to:
  - Development engineers
  - Engineering managers
  - Regulators
  - Society at large
  - Etc.
- Many industries rely on standards for many reasons
- So do many regulators

Benefits of Standards

Given their benefits, perhaps a little reflection on the mechanism is worthwhile

Role of Standards

- Standards underlie much of safety engineering
- Standards are not themselves a technology
- Standards set a direction that has to be followed if compliance is to be claimed



Roles Standards Play

- Standards help to define certifying organization’s:
  - Intent
  - Expectations
- Define technical approach:
  - In many cases, standards ensure that appropriate technical approaches are used
- Education:
  - Standards educate those subject to the standard
  - Many are unfamiliar with the spectrum of technical issues that have to be addressed
  - *Standards integrate the knowledge and experience of many*

Compliance With Standards

- Successful compliance with a standard requires deep understanding of:
  - Technology
  - Goals
  - Intent of the standard
- Such depth and breadth are unlikely to be in the experience of all involved in safety-critical systems development
- Standards itemize the many applicable techniques and technologies

But…

Standards have their problems:

- Development processes tend to be:
  - Informal and ad hoc
  - Conducted by those to whom standard will apply
- Standards are inaccessible
- Multiple standards address the same topic
- Texts of standards tend to be imperfect/unclear
- Compliance/conformance is usually undefined
- Standards tend not to be maintained

An Example – MIL STD 882E

DEPARTMENT OF DEFENSE STANDARD PRACTICE
SYSTEM SAFETY

Appendix B: 2.2.5.a - Software system safety requirements and tasks: Design requirements

Design requirements to consider **include** fault tolerant design, fault detection, fault isolation, fault annunciation, fault recovery, warnings, cautions, advisories, redundancy, independence, **N-version design**, functional partitioning (modules), physical partitioning (processors), design safety guidelines, design safety standards, and **best and common practices**.

An Example – RTCA DO-178B

Software Considerations In Airborne Systems And Equipment Certification

- Published 1992, in effect until February 2012
- Section 4.4 - Software Life Cycle Environment Planning:

The goal of error prevention methods is to avoid errors during the software development processes that might contribute to a failure condition. The basic principle is to **choose requirements development and design methods, tools, and programming languages that limit the opportunity for introducing errors**, and verification methods that ensure that errors introduced are detected.

Systematically Ignored

An Example – RTCA DO-178B

OK, time for a revision

- FAA asked RTCA to form committee to prepare revision:
  - Not an FAA committee although FAA had membership
  - Committee management by volunteers, no payment
  - Committee membership open to all
  - New standard will essentially define software certification mechanism
- RTCA formed Special Committee (SC) 205

From The SC 205 Terms of Ref

8. OTHER CONSIDERATIONS

Reference:

1. Maintain the current ***objective-based*** approach for software assurance.
2. Maintain the technology independent nature of the DO-178B objectives.
3. Evaluate issues as brought forth to the SCWG. For any candidate guidance modifications determine if the issue can be satisfied first in guideline related documents.

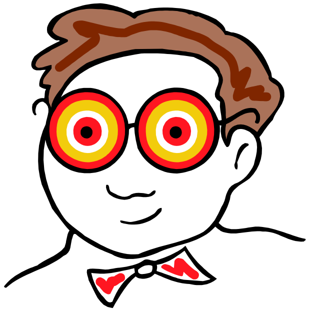
From The SC 205 Terms of Ref

4. Modifications to DO-178B/ED-12B should:

1. **Strive to minimize changes to the existing text** (i.e., objectives, activities, software levels, and document structure).
2. **Consider the economic impact** relative to system certification without compromising system safety.
3. Address clear errors or inconsistencies in DO-178B/ED-12B
4. Fill any clear gaps in DO-178B/ED-12B
5. Meet a documented need to a defined assurance benefit.

Thesis

The time has come for **standards** to be held to a higher **standard**



IEC
ISO
IEEE
SAE
RTCA

Standard for Standards – SfS

- □ The SfS maintains established benefits
- □ Adds additional benefits
- □ Eliminates some of the difficulties that standards present

The S f S

Technical Peer Review

Linguistic Peer Review

Empirical Assessment

Proactive Maintenance

Value-Based Funding

Technical Peer Review

- Standards are technical documents
- Independent peer review is a basic requirement
- Public comment approach is ad hoc, ineffective
- Review committee should:
  - Be composed of independent experts
  - Be funded by the standards organization
  - Be involved from the beginning of the standard development process
  - Be named as part of the standard
- Peer review of standards should be prestigious

Linguistic Peer Review

- Text has to be:
  - Clear
  - Unambiguous
  - Complete
- Achieving these qualities is difficult
- Linguists and other experts know how to achieve these qualities
- Experts should be consulted

Empirical Assessment

- Standards result from human deliberation
- Are those deliberations fault free?
- Probably not – see DO-248:

Final Report for Clarification of DO-178B "Software Considerations in Airborne Systems and Equipment Certification”

- Societal dependence on standards suggests that more care would be valuable
- Empirical assessment:
  - Apply standard in “laboratory” before final publication
  - Assess efficacy and utility
  - Repair as necessary

Proactive Maintenance

- Standards upon which systems are based need regular maintenance
- DO-178B example:
  - Originally published in 1992
  - Regular guidance and supplements issued
  - Incomprehensible and ineffective as a result
- Importance of standards suggests:

Set a maximum lifetime of five years

Value-Based Funding

- Access to standards is severely limited by price in most cases
- Examples:

DO-178C	$290
IEC 61508 Edition 2	$2743

- Standards cannot be:
    - Examined before use – what other product is like that?
    - Used in education – try that with the calculus
- Yet in many domains, such standards are required

Value-Based Funding

- Proposal (and I ***really*** mean this):

Fees should be returned to standards publishers based on value to user, not artificial cost of a copy

- Approach:
  - All standards documents should be freely available at no charge
  - Fees returned to publisher for claiming compliance:
    - Submission to a regulating agency
    - Public claim to promote product
  - No change in certification process

Conclusion

- Utility and merit of standards is not in question
- Concerns are:
  - Content of some standards
  - Development process of standards
  - Maintenance process of standards
  - Accessibility of standards
- These issues need to be addressed